



# METHOD AND APPARATUS FOR PROCESSING CRYPTOGRAPH IN COMMUNICATION CIRCUIT NETWORK USING SINGLE CRYPTOGRAPHIC ENGINE

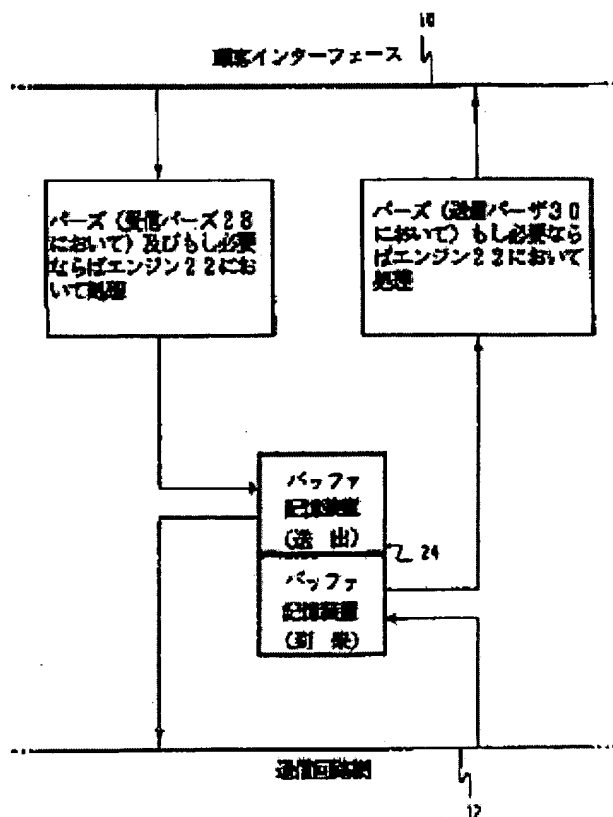
**Patent number:** JP5199220  
**Publication date:** 1993-08-06  
**Inventor:** FUJITSUPU PINCHIYAAZU ROZOBUI; SHIIMAN TOBU BEN MAIKERU  
**Applicant:** DIGITAL EQUIPMENT CORP  
**Classification:**  
 - international: G09C1/00; H04L9/00; H04L9/10; H04L9/12  
 - european: H04L29/06  
**Application number:** JP19920156793 19920616  
**Priority number(s):** US19910722745 19910628

Also published as:

 EP0525968 (A2)  
 EP0525968 (A3)

## Abstract of JP5199220

**PURPOSE:** To provide a simple device which uses a single cipher engine to perform the cipher processing of data transferred between a customer interface and a communication circuit network bidirectionally. **CONSTITUTION:** An output data packet received from a customer interface 10 is immediately parsed by a means 28 to determine whether the cipher processing is requested or not; and if it is requested, a proper part of the packet is subjected to the cipher processing at the time of reception of the packet and is stored in a transmission buffer storage device 24 till transferred onto a communication circuit network 12. A data packet from the communication circuit network 12 is not immediately parsed, and it is stored in an arrival buffer storage device 24 until the customer interface is made available. Parsing and the required cipher processing of the arriving packet are not performed until the customer interface is made available and it is retrieved from the arrival buffer storage device for transfer. Only a single cipher engine is required for a half-duplex customer buffer.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平5-199220

(43) 公開日 平成5年(1993) 8月6日

(51) Int.Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00				
	9/10			
	9/12			
G 0 9 C 1/00		9194-5L	H 0 4 L 9/00	Z
		7117-5K	審査請求 未請求 請求項の数15(全 11 頁)	

(21) 出願番号 特願平4-156793

(22) 出願日 平成4年(1992) 6月16日

(31) 優先権主張番号 07/722745

(32) 優先日 1991年6月28日

(33) 優先権主張国 米国 (US)

(71) 出願人 590002873

デジタル イクイブメント コーポレイ  
ション

アメリカ合衆国 マサチューセッツ州

01754メイナード メイン ストリート

146

(72) 発明者 フィリップ ビンチャーズ ロゾヴィック  
イスラエル エルサレム フランクフルテ  
ル ストリート 2

(72) 発明者 シーマン トヴ ベン マイケル  
イスラエル ギラト ゼール ミッツベ  
ストリート 1313

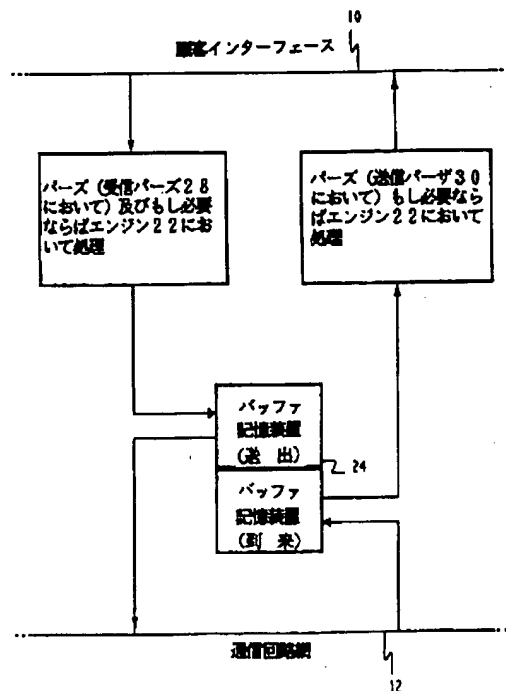
(74) 代理人 弁理士 中村 稔 (外6名)

(54) 【発明の名称】 単一の暗号エンジンを使用する通信回路網内の暗号処理方法及び装置

(57) 【要約】 (修正有)

【目的】 “顧客” インタフェースと通信回路網間で両方向に転送されるデータを単一の暗号エンジンを使用して暗号処理する簡便な装置を提供する。

【構成】 顧客インタフェース10から受信した出力データパケットは、暗号処理の要求の有無の決定のために直ちにパーズ28され、要求されていればパケットを受信した時にその適切な部分が暗号処理され、通信回路網上へ転送されるまで送出バッファ記憶装置24内に記憶される。通信回路網12からのデータパケットは直ちにパーズされず、顧客インタフェースが使用可能になるまで到来バッファ記憶装置24内に記憶される。到来パケットのパーキング及び必要暗号処理は、顧客インタフェースが使用可能になり、転送のため到来バッファ記憶装置から検索されるまで遂行されない。半二重顧客バッファは単一の暗号エンジンだけが要求される。



## 【特許請求の範囲】

【請求項1】 半二重顧客インタフェースから通信回路網へ送出されるデータと、通信回路網から顧客インタフェースへ到来するデータとを暗号エンジン手段を使用して暗号処理する方法であって、

送出データパケットを顧客インタフェースから受信した時に、もし必要ならば、唯一の暗号エンジンを使用して暗号処理する段階と、

到来データパケットが顧客インタフェースへ送信されて来た時に、もし必要ならば、上記唯一の暗号エンジンを使用して暗号処理する段階と、

到来データパケットと送出データパケットとを転送する前に、必要に応じて、一時バッファ記憶装置内に記憶する段階と、

を具備し、顧客インタフェースが送出データパケットと到来データパケットとを同時に処理することができないために、単一の暗号エンジンだけしか必要としないことを特徴とする方法。

【請求項2】 処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各送出データパケットをパーズする段階と、

処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各到来データパケットをパーズする段階とをも具備する請求項1に記載の方法。

【請求項3】 到来パケットと送出パケットとを一時バッファ記憶装置内に記憶する段階が、もし顧客インタフェースが使用不能であれば到来パケットを記憶する段階と、

もし通信回路網が使用不能であれば送出パケットを記憶する段階とを含む請求項1に記載の方法。

【請求項4】 ループバックパケットを顧客インタフェースから受信する段階と、

ループバックパケットを、もし必要ならば、直ちにパーズし、暗号処理する段階と、

もし顧客インタフェースが使用不能であればループバックパケットを記憶する段階とをも具備する請求項3に記載の方法。

【請求項5】 半二重顧客インタフェースから通信回路網へ送出されるデータと、通信回路網から顧客インタフェースへ到来するデータとを単一の暗号エンジンだけを使用して暗号処理する方法であって、

通信回路網から到来するデータパケットを受信する段階と、

受信した各パケット毎に顧客インタフェースが使用可能か否かを決定する段階と、

もし顧客インタフェースが使用不能であれば、顧客インタフェースが使用可能になるまで到来データパケットを記憶し、次いでそのパケットを検索する段階と、

データパケットを暗号処理すべきか否かを決定するため

にパーズし、もし必要ならば、単一の暗号エンジンを使用してそのパケットを暗号処理し、そのパケットを顧客インタフェースへ送信する段階と、

顧客インタフェースから送出されるデータパケットを受信する段階と、

顧客インタフェースから受信した各パケットをパーズする段階と、

もし先行パージング段階によって処理が必要であると決定されていれば、顧客インタフェースから受信した各パケット毎に上記単一の暗号エンジンを使用して暗号処理する段階と、

通信回路網が使用可能であるか否かを決定する段階と、もし通信回路網が使用不能であれば、通信回路網が使用可能になるまで各送出データパケットを記憶し、次いでその送出パケットを検索する段階と、

送出データパケットを通信回路網上に送信する段階とを具備し、送出パケットの暗号処理をそれらのパケットが顧客インタフェースから受信した時に遂行し、また到来パケットの暗号処理をそれらのパケットが顧客インタフェースへ送信する時に処理するが、顧客インタフェースの半二重動作がこれらの両機能の同時発生の可能性を妨げるために、データの暗号処理の諸段階を遂行するには単一の暗号エンジンで十分であることを特徴とする方法。

【請求項6】 ループバックパケットを顧客インタフェースから受信する段階と、

ループバックパケットを、もし必要ならば、直ちにパーズし、暗号処理する段階と、

もし顧客インタフェースが使用不能であればループバックパケットを記憶する段階とをも具備する請求項5に記載の方法。

【請求項7】 パケットを顧客インタフェースへ送信するのに先立って、

顧客インタフェースが使用可能になる前にパケットの一部をパーズする段階と、

パケットのパーズされた部分を先入れ先出しバッファ内に記憶して送信準備を整える段階と、

同一パケットの付加的なデータを先入れ先出しバッファ内に記憶し、該バッファから検索しながら、検索されたデータを顧客インタフェース上へ送信開始する段階とをも具備する請求項5に記載の方法。

【請求項8】 半二重顧客インタフェースから通信回路網へ送出されるデータと、通信回路網から顧客インタフェースへ到来するデータとを単一の暗号エンジンだけを使用して暗号処理する装置であって、

送出データパケットを顧客インタフェースから受信した時に、もし必要ならば、及び到来データパケットが顧客インタフェースへ送信されて来た時に、もし必要ならば、暗号処理する単一の暗号エンジンと、

到来データパケットと送出データパケットとを転送する

前に、必要に応じて、記憶するバッファ記憶装置手段と、  
を具備し、顧客インタフェースが送出データパケットと  
到来データパケットとを同時に処理することができない  
ために単一の暗号エンジンだけしか必要としないことを  
特徴とする装置。

【請求項9】 処理が必要か否かを決定し、また遂行す  
べき処理の型を決定するために暗号処理の直前に各送出  
データパケットをパーズする手段と、

処理が必要か否かを決定し、また遂行すべき処理の型を  
決定するために暗号処理の直前に各到来データパケット  
をパーズする手段とをも具備する請求項8に記載の装  
置。

【請求項10】 バッファ記憶装置手段が、  
もし顧客インタフェースが使用不能であれば到来パケ  
ットを記憶する手段と、

もし通信回路網が使用不能であれば送出パケットを記憶  
する手段とを含む請求項9に記載の装置。

【請求項11】 顧客インタフェースが使用可能になる  
まで顧客インタフェースから受信したループバックパケ  
ットを記憶し、必要に応じて、暗号エンジン内において  
暗号処理する手段をも具備する請求項10に記載の装  
置。

【請求項12】 半二重顧客インタフェースから通信回  
路網へ送出されるデータと、通信回路網から顧客インタ  
フェースへ到来するデータとを単一の暗号エンジンだけ  
を使用して暗号処理する装置であって、

通信回路網から到来データパケットを受信する手段と、  
顧客インタフェースが使用可能か否かを決定する手段  
と、

もし顧客インタフェースが使用不能であれば、各到来デ  
ータパケットを記憶する手段と、

顧客インタフェースが使用可能になると作動可能にな  
り、記憶されたデータパケットを検索する手段と、

到来データパケットを暗号処理すべきか否かを決定す  
るためにそのデータパケットをパーズする手段と、

もし必要ならば、到来データパケットを暗号処理する  
ように作動可能な暗号エンジンと、

到来データパケットを顧客インタフェースへ送信する  
手段と、

顧客インタフェースから送出データパケットを受信する  
段階と、

顧客インタフェースから受信した各パケットをパーズ  
し、もし必要ならば、各パケットを処理するために暗号  
エンジン内へ転送する手段と、

通信回路網が使用可能であるか否かを決定する手段と、  
もし通信回路網が使用不能であれば、各送出データパ  
ケットを記憶する手段と、

通信回路網が使用可能になると作動可能になり、記憶  
されたデータパケットを検索し、それを通信回路網へ送信

する手段と、

を具備し、送出パケットの暗号処理をそれらのパケット  
が顧客インタフェースから受信した時に遂行し、また到  
来パケットの処理をそれらのパケットが顧客インタフェ  
ースへ送信する時に処理するが、顧客インタフェースの  
半二重動作がこれらの両機能の同時発生の可能性を妨げ  
るためにデータの暗号処理を遂行するには単一の暗号エ  
ンジンで十分であることを特徴とする装置。

【請求項13】 ループバックデータパケットを記憶す  
る手段をも具備し、送出パケットを受信しパーズする  
手段が、ループバックパケットを顧客インタフェースから  
受信するとこれらのループバックパケットを受信しパー  
ズするようにも働き、また暗号エンジンが、必要に応じ  
て、ループバックパケットを暗号処理するようにも働く  
請求項12に記載の装置。

【請求項14】 データパケットを記憶する手段に対す  
る双方向アクセスを提供する高速データベースをも具備  
する請求項13に記載の装置。

【請求項15】 到来データパケットの一部分を、顧客  
インタフェースへ送信する前に記憶する先入れ先出しバ  
ッファと、

顧客インタフェースが使用可能になる前に先入れ先出し  
バッファ内に記憶されているパケットの一部分のパージ  
ングを開始して送信準備を整える手段と、

顧客インタフェースが使用可能になると先入れ先出しバ  
ッファからデータを検索し、同一パケットの付加的なデ  
ータを先入れ先出しバッファ内に記憶し、該バッファか  
ら検索しながら、検索されたデータの顧客インタフェ  
ース上への送信を開始する手段とをも具備する請求項12  
に記載の装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、一般的には通信回路網  
における暗号処理に関する。具体的には、通常は比較的  
ローカルなコンピュータ及び他の装置の回路網であるユ  
ーザまたは“顧客”インタフェースと、選択された宛先  
へ顧客インタフェースからメッセージを伝送する通信回  
路網との間に配置される暗号装置に関する。

【0002】

【従来の技術】 多くの他のシステム及び顧客が通信回路  
網への合法的なアクセスを有しているから、これらの伝  
送の安全性が屢々重要な問題となる。異なる回路網プロ  
トコル層における動作のための種々の通信安全プロトコ  
ルが開発されている。これらの安全プロトコルの本質の  
詳細は、どのような所望の安全プロトコルを取り扱うこ  
ともできる本発明にとっては重要ではない。

【0003】 本発明が関係する安全サービスの原理的な  
型は、機密性のための暗号と、完全性のための暗号とを  
含む。機密性とは、発信者から無許可の個人または構成  
要素へ情報が伝送されないように保護することである。

この目的のために、情報は伝送される前に暗号化された形状に変換され、宛先において受信されると“解読された本文”形状に解読される。完全性とは、受信したデータが伝送中に変更されたか否かを検出することを含む。この目的のためには情報を暗号化する必要はなく、単に伝送経路の各端において独特な暗号検査合計を発生させるような処理を行うに過ぎない。もし検査合計が整合しなければ、当該データは変更されたものと見做される。

【0004】理想的には、暗号処理はユーザまたは顧客に対して“透明”にすべきである。そのようにすればメッセージの送受信を、暗号処理の性質に、またはその存在にさえ関係することなく遂行することができ、その使用が“待ち時間”と呼ばれる伝送遅延時間を大幅に増大させたり、または“処理能力”即ち顧客と回路網との間のデータの流れのレートに重大な影響を与えたりすることはなくなる。しかしながら完全に透明な暗号処理は複雑でもあり、また費用もかかる。従って、顧客インタフェースに接続されている各関連装置が暗号処理のある面に対する責を負っているような費用のかからない非透明暗号処理技術が要望されている。

【0005】回路網に使用する暗号システムを設計する場合の重要な目標は、データパケットが何れの方角に通過しようとも重大な遅延をもたらさない“オンザフライ”で処理を遂行できるように、暗号処理を顧客インタフェースと通信回路網との間に配置すべきことである。若干の形態においては暗号処理を顧客インタフェース制御装置内に組み入れることができるが、それでも暗号処理は通信経路において遂行される。データは、暗号装置を通して両方向に伝送しなければならないから、殆どの従来装置は両方向のデータ流を同時に処理するために2つの独立暗号エンジンを使用していた。単一の暗号エンジンを使用すると一方の、または他の方向の処理に遅延を生じさせることによって性能に悪影響を与えるものと広く信じられている。

【0006】従って、回路網通信の暗号処理の分野における改善が未だに要望され、特に、従来装置の性能を低下させないような低価格装置、即ち単一の暗号エンジンだけしか必要としない装置が要望されている。本発明はこの要望を満足させるものである。

【0007】

【発明の概要】本発明は、単一の暗号エンジンだけを使用するが、2つの暗号エンジンを使用する装置に比して通信の処理能力または待ち時間に何等の悪影響をもたらさない暗号インタフェースを通信回路網と半二重顧客インタフェースとの間に設けた暗号処理装置、及び関連する方法を提供する。要約すれば、そして一般的に表現すれば本発明の方法は、送出されるデータパケットを顧客インタフェースから受信した時に、もし必要ならば、唯一の暗号エンジンを使用して暗号処理する段階と、到来データパケットが顧客インタフェースへ送信されて来た

時に、もし必要ならば、上記唯一の暗号エンジンを使用して暗号処理する段階と、到来データパケットと送出データパケットとを転送する前に、必要に応じて、一時バッファ記憶装置内に記憶する段階とからなる。殆どの場合には、データパケットは“カットスルー”動作と呼ばれる動作で直ちに転送されよう。顧客インタフェースが送出パケットと到来パケットとを同時に処理することができないために、単一の暗号エンジンだけしか必要としない。

【0008】本方法は、処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各送出データパケットをパース（または構文解析）する段階と、処理が必要か否かを決定し、また遂行すべき処理の型を決定するために暗号処理の直前に各到来データパケットをパースする段階とをも含むことが好ましい。到来パケットと送出パケットとを一時バッファ記憶装置内に記憶する段階は、もし顧客インタフェースが使用不能であれば到来パケットを記憶する段階と、もし通信回路網が使用不能であれば送出パケットを記憶する段階とを含む。

【0009】本発明の方法は、ループバックパケットを顧客インタフェースから受信する段階と、ループバックパケットを、もし必要ならば、直ちにパースし、暗号処理する段階と、もし顧客インタフェースが使用不能であればループバックパケットをループバックバッファ記憶装置内に記憶する段階とをも含むことができる。以下に説明するように、本発明の好ましい実施例は、通信回路網から到来するデータパケットを受信する段階と、顧客インタフェースが使用可能か否かを決定する段階と、使用不能であれば、到来各データパケットを到来バッファ記憶装置内に記憶する段階を含む。次いで顧客インタフェースが使用可能になると、本方法は記憶されたデータパケットを検索する段階を含む。これに続くのは、データパケットを暗号処理すべきか否かを決定するためにパースし、もし必要ならば、パケットを暗号処理し、そのパケットを顧客インタフェースへ送信する段階である。他方向におけるトラフィックに対しては本方法は、顧客インタフェースから送出されるデータパケットを受信する段階と、顧客インタフェースから受信した各パケットをパースする段階と、もし処理が必要であると決定されれば、顧客インタフェースから受信した各パケットを暗号処理する段階と、通信回路網が使用可能であるか否かを決定する段階とを含む。もし通信回路網が使用不能であれば本方法は、各送出されるデータパケットを記憶する段階と、回路網が使用可能になるとデータパケットを検索する段階を含む。本方法の最終段階は、送出されるパケットを通信回路網上に送信することである。

【0010】送出パケットを顧客インタフェースから受信した時に送出パケットの暗号処理が遂行され、また到

来パケットを顧客インタフェースへ送信する時に到来パケットの暗号処理が遂行されるので、データの両暗号処理段階を遂行するには単一の暗号エンジンで十分である。顧客インタフェースの半二重動作が、これらの両機構を同時に要求する可能性を妨げる。

【0011】ループバックパケットを処理することに関して本方法は、ループバックパケットを顧客インタフェースから受信する段階と、ループバックパケットを、もし必要ならば、直ちにパーズし、暗号処理する段階と、もし顧客インタフェースが使用不能であればループバックパケットを記憶する段階とを含む。本発明の別の面によれば、方法は更に、顧客インタフェースが使用可能になる前に到来データパケットの一部分をパーズする段階と、パケットのパーズされた部分を先入れ先出しバッファ内に記憶して送信準備を整える段階と、顧客インタフェースが使用可能になると先入れ先出しバッファからデータを検索する段階と、同一パケットの付加的なデータを先入れ先出しバッファ内に記憶し、該バッファから検索しながら、検索されたデータを顧客インタフェース上へ送信開始する段階とを含む。先入れ先出しバッファを使用することによって、インタフェースが使用可能になった直後に、遅延を伴わずに顧客インタフェース上への送信が開始されるようになる。

【0012】新しい装置に関しては本発明は、その最も広義の表現では、送出データパケットを顧客インタフェースから受信した時に、もし必要ならば、及び到来データパケットが顧客インタフェースへ送信されて来た時に、もし必要ならば、暗号処理する単一の暗号エンジンと、到来データパケット及び送出データパケットを転送する前に、必要に応じて、記憶するバッファ記憶装置手段とを含む。前述のように、顧客インタフェースが送出データパケットと到来データパケットとを同時に処理することができないから、この目的のためには単一の暗号エンジンで十分である。本発明の装置は、ループバックデータパケットを記憶する手段をも含むことができ、また上述した種々の形状を有する本発明の方法の範囲に対比できる他のより特定の表現によって限定することもできる。

【0013】以上の説明から、本発明が回路網通信に使用するための暗号処理の分野に重要な進歩をもたらしていることが明白になったであろう。即ち本発明は、単一の暗号エンジンを使用しながら2つの暗号エンジンを使用する装置に比して処理能力または待ち時間を何等劣化させることなく、通信回路網と顧客インタフェースとの間の双方向暗号処理を提供する。

【0014】以下に添付図面に基づいて本発明の好ましい実施例を説明するが、この説明から本発明がより明白になるであろう。

【0015】

【実施例】例として添付図面に示すように、本発明は顧

客インタフェースと通信回路網との間を両方向に通過するデータパケットを暗号処理する装置に関する。従来は、最小の遅延で両方向のトラフィックを効率的に処理するためには、少なくとも2つの独立的に作動する暗号エンジンを含む必要があるものと考えられていた。本発明以前には、単一の暗号エンジンを使用すると必然的に待ち時間または処理能力にある種の性能低下がもたらされるものと考えられて来た。

【0016】本発明によれば、装置の待ち時間または処理能力に重大な影響を与えることなく、顧客インタフェースと通信回路網との間で両方向の暗号処理をするために単一の暗号エンジンを使用する。この目標を単一の暗号エンジンを用いて達成することは不可能に見えるかも知れないが、もし顧客インタフェース内の通信媒体へのアクセスのために使用されるプロトコルが、一般にキャリア検知多重アクセス/衝突検出(CSMA/CD)と呼ばれるプロトコルを使用するイーサネットのような半二重媒体であれば、可能である。回路網バスまたはケーブルへのアクセスのためのCSMA/CD規約の下では、送信を望んでいるどのステーションも、送信を開始する前にそのケーブルが話し中でないことを確認するために先ず“聴守”しなければならない。回路網上の全てのステーションは平等のアクセス優先順位を有しており、ラインが話し中でなくなると直ちに、そして何等のパケット間遅延も要求されることなく送信を開始することができる。しかしながら、もし送信を開始した第1のステーションが別のステーションからの送信との“衝突”を検出すれば、第1のステーションは短い時間の間にわたって送信を継続し、送信を望んでいる全ステーションに衝突を検出させる。次いで第1のステーションはランダムな時間の後に送信を終了する。衝突に関与している他のステーションは同じことはせず、送信の再開を試みる前にランダムな、従って通常は異なる遅延時間を選択する。

【0017】回路網アクセスに関するCSMA/CD規約は、全二重伝送を、即ち同時に送受信することを許容しないようになっている。もしあるステーションがメッセージを受信中であれば回路網は話し中であり、このステーションまたは他のどのステーションからも送信を開始することはできない。同様に、もしこのステーションから送信が進行中であれば、このステーションがメッセージを送っている間は他のステーションは回路網にアクセスを得ることはできないので、同時にメッセージを受信することはできない。従って、イーサネットまたは他のCSMA/CDステーションの動作の性質は半二重、即ちメッセージの送信及び受信の両方を同時に行うことはできないが、回路網アクセス規約の性質から、同時になければ可能である。イーサネット及びCSMA/CDのこの特性が本発明に、特定的には顧客インタフェース内に使用され、単一の暗号エンジンを通して、2つの暗

号エンジンを使用する装置に比して待ち時間または処理能力に何等の劣化を与えることなく、メッセージの双方向伝送を提供する。しかしながら、本発明はCSMA/CDとの併用に限定されるものではなく、どのような半二重通信媒体とも同じように動作することは明白である。

【0018】図1は顧客インタフェース10と通信回路網12との間に接続されている実施例の装置を簡易ブロック線図で示している。以下の説明では、顧客インタフェースに関連する装置の面を装置の“顧客側”と呼ぶことがあり、また通信回路網に関連する装置の面を装置の“回路網側”と呼ぶことがある。装置の関連成分は、顧客受信装置(RxC)14、顧客送信装置(TxC)16、回路網受信装置(RxN)18、回路網送信装置(TxN)20、単一の暗号エンジン22、バッファ記憶装置24、顧客送信FIFO記憶装置26、受信バーザ28及び送信バーザ30を含む。

【0019】これらの成分は、特定の時点に処理するトラフィックの型に依存して種々の論理構成に接続される。説明する全ての経路はバッファ記憶装置24を通過しているが、バッファ記憶装置をデータパケット記憶装置としてではなく、各データ経路の一部として使用する2つの直接論理経路が存在する。第1に、顧客インタフェース10から回路網ケーブル12までの直接論理経路が存在する。この経路は顧客インタフェース10から顧客受信装置14までの線32と、顧客受信装置から(バッファ記憶装置24を介して)回路網送信装置20までの線34と、回路網送信装置から回路網ケーブル12までの第3の線36とを含む。同様に、通信回路網12から顧客インタフェース10までの別の直接論理経路は、通信回路網から回路網受信装置18までの線38と、回路網受信装置から(バッファ記憶装置24を介して)顧客送信FIFO記憶装置26までの線40と、FIFO記憶装置から顧客送信装置16までの別の線42と、顧客送信装置から顧客インタフェース10までのさらなる線44とを含む。実際には論理的に分離している3つの記憶装置であるバッファ記憶装置24は、データバス46によって、線34に沿う“送出”データ経路と、線40に沿う“到来”データ経路とに接続されている。

【0020】以上のデータ経路の説明からバッファ記憶装置24は、データパケットを直ちに送信できない場合にはそれらを記憶するように働き、また全パケットを記憶することなくデータを直ちに転送するようにも働くことが理解されよう。これらの両動作は、技術的には記憶装置内にデータを“記憶”することを含むが、この説明では“記憶”と言う語は全データパケットが爾後に通信回路網または顧客インタフェース上へ転送するために保持するような状況のために保留する。“カットスルー”動作モードにおいてデータパケットがバッファ記憶装置を通過する場合には、あるパケットの一部がまだ

記憶装置に到着しつつある間にもそのパケットは既に記憶装置から送信されている。

【0021】双方向トラフィックの見掛け上の同時処理に対する鍵は、図2のデータ流れ図を参照すると理解し易い。顧客インタフェース10から受信されるデータパケットは、それが受信されると受信バーザ28によって必ずバーザされ、受信バーザ28内におけるバージング処理から暗号処理が必要であることが決定されると、エンジン22によって暗号処理される。次いで暗号処理がなされている、いないに拘わらず、データパケットは、通信回路網12へのアクセスを待機する必要がある限りバッファ記憶装置24内に記憶される。これに対して、通信回路網12から受信したデータパケットは直ちにバーザまたは暗号処理されることなく、先ず一時的に記憶するためにバッファ記憶装置24に導かれる。通常は、顧客インタフェースは使用可能であり、パケットは直ちにバッファ記憶装置から検索されよう。実際に通常はパケットは、それがまだ通信回路網12から受信中でも顧客インタフェースへ送信されることになる。これは、もし顧客インタフェースが使用不能であれば全パケットを一時記憶装置内に保持する“蓄積転送”動作に対して、“カットスルー”動作として知られている。何れの場合も、顧客インタフェースが使用可能であるか、または後刻使用可能になれば、パケットはバッファ記憶装置24から送給され、送信バーザ30によってバーザされ、もし必要ならばエンジン22によって暗号処理され、そして最後に顧客インタフェース10へ転送される。暗号エンジン22は、使用することが要求されると、顧客インタフェース10から受信されているデータパケットを処理するか、または顧客インタフェース10へ送信されて来たデータパケットを処理するの何れかを遂行する。もし顧客インタフェースが既に話中でデータパケットを装置へ送給していれば送出パケットのバージング及び考慮得る暗号処理は開始されないから、エンジン22のこれら2つの機能が同時に要求されることはあり得ない。

【0022】詳述すれば、回路網受信装置18によって通信回路網12から受信されたデータパケットは直接バッファ記憶装置24へ転送される。もし顧客インタフェース10が現在パケットを送信または受信していなければ、そのパケットは顧客送信FIFO記憶装置26に転送され、また並列に送信バーザ30によってバーザされる。もし必要ならば、バーザによって決定された適切なバイトから、データは顧客送信FIFO記憶装置26に転送される前に暗号エンジン22を通過させられる。最後に、顧客送信装置16はデータを顧客送信FIFO記憶装置26から引き出し、データパケットを顧客インタフェース10へ送信する。

【0023】通信回路網12から受信されたパケットがバッファ記憶装置24へ入った場合には、もし現在パケットを顧客インタフェース10から受信してはいるが、

顧客インタフェースへ送信すべき未処理バケットが存在していなければ、そのバケットの始めの部分は、あたかもそれが送信されるもののように顧客送信FIFO記憶装置26へ転送され、その始めの部分のバージングが遂行される。しかし、顧客インタフェースはまだ話し中であると見られるから暗号処理が開始されることはなく、また顧客送信装置16が顧客送信FIFO記憶装置26からデータを引き出すこともない。顧客送信FIFO記憶装置26が一杯になると、実際の送信が開始され顧客送信装置16が顧客送信FIFO記憶装置26からデータを引き出し始めるまで、それ以上のデータは転送されない。FIFO記憶装置のこのプリローディングは、暗号エンジン22が動作し始める時に、そしてそれがデータの第1ブロックを処理し、エンジンのデータの“パイプライン”が安定状態に達するまで、データの“アンダーラン”が送信されないようにする。

【0024】図3は、本発明の装置をより詳細に示す図である。図3には示されているが、図1及び2の簡易図には示されていない成分は、バッファ記憶装置24を制御する記憶装置制御装置50と、顧客受信制御論理回路(CRCTL)52と、顧客送信制御論理回路(CTCTL)54と、バケット制御論理回路56と、4つの直接メモリアクセスユニット(CRDMA 57、NTDMA 58、CTDMA 60及びNRDMA 62)と、3つの付加FIFO記憶装置(CRFIFO 64、NTFIFO 66及びNRFIFO 68)とを含む。これらの付加的な成分の機能について以下に概要を説明する。

【0025】顧客受信制御論理回路(CRCTL)52は装置の顧客側の受信動作(受信バーザ28及び暗号エンジン22の動作の調整を含む)を制御する。顧客送信制御論理回路(CTCTL)54は、装置の顧客側の送信動作(送信バーザ30及び暗号エンジン22の動作の調整を含む)を制御する。付加FIFO記憶装置64、66、68は比較的小さい記憶装置であり、その主目的はデータバス46の効率的な動作のためのバッファとなることである。DMAユニット57、58、60、62はバッファ記憶装置24にアクセスするための普通のDMA機能を提供する。記憶装置制御装置50は、バッファ記憶装置の動作とデータバス46上での関連動作とを管理する。最後に、バケット制御論理回路56は、データの緩衝要求を最小にするように、装置の顧客側及び回路網側への、及びこれらの側からのデータ流を調整する。

【0026】装置の顧客側から回路網側への送出データ流の場合のバージングは、バケットがデータバス46を通してバッファ記憶装置24へ転送されるのと同時に到来データバケットに対して(受信バーザ28において)遂行される。バケットに対して暗号処理が要求されていることを受信バーザ28が検出すると、バーザ28はそ

れを顧客受信制御論理回路(CRCTL)52に通知し、顧客受信制御論理回路52は適切な時点でデータを顧客受信装置14から暗号エンジン22内へ導き始める。暗号処理の後に、データバケットはバッファ記憶装置24内に記憶される。装置の回路網側がデータバケットを受け入れ可能になると、回路網の可用性に依存して、バケット制御論理回路56は回路網送信装置に送信を開始するように指令し、データをバッファ記憶装置24から回路網送信装置へ、次いで通信回路網上へ転送する。カッスルーと呼ばれるこの動作は、装置の顧客側からのデータの連続受信と同時に遂行させることが可能である。

【0027】装置の回路網側から顧客側への到来データ流は直ちにパースされずに、回路網受信装置18からバッファ記憶装置24へ直接転送される。装置の顧客側が使用可能になると、バケット制御論理回路56はバケット制御論理回路56に指令して顧客側への転送を開始させる。この動作は回路網側からのデータの受信と同時に遂行させることが可能である。データのバケットが顧客送信FIFO26へ送られ始めると、それは同時に送信バーザ30によってパースされる。暗号処理動作が要求されていることを送信バーザ30が検出すると、それは顧客送信制御論理回路(CTCTL)54に通知され、顧客送信制御論理回路54は適切な時点でデータ流を顧客受信装置14から暗号エンジン22内へ導き、データバケットは暗号エンジン22から顧客送信FIFO26を通して顧客インタフェースへ流れる。

【0028】到来データバケット及び送出データバケットの他に、装置はループバックデータバケットをも処理する。ループバックデータバケットは、装置の顧客側から受信され、通常は暗号処理後に顧客側に戻されるデータのバケットである。ループバック機能によって顧客装置は、データバケットの“ローカル”暗号処理が可能になる。ループバック動作は、ファイル暗号文のような暗号サービスを顧客に提供する。ループバック機能は、例えばもし到来データバケットが、遂行されるべきではない時点で偶発的に解読されるか、または到来バケットを解読すべきであるのに解読されていない場合にも必要である。基本的には、ループバック機能は送出バケットではないデータバケットの暗号処理へのアクセスを顧客に与える。装置の顧客側から受信したループバックバケットは、送出バケットと殆ど同じようにして処理される。それらはバッファ記憶装置24への途上でパースされるが、送出バッファの代わりに、バッファ記憶装置のループバックバッファ内に記憶される。ループバックバケットを顧客に送り返す時点、即ち顧客側が使用可能でありループバックバケットを送信する転機である時点になると、バケットは何等の付加的な処理も受けずに顧客に直接送り返される。

【0029】受信バーザ28及び送信バーザ30におい



13

て遂行される特定のパーズング手順は、回路網プロトコル及び使用する特定のデータパケットフォーマットに大きく依存し、本発明の一部であるとは考えていない。パーズングは、あるデータパケットに対して暗号処理が必要か否かを決定するために、単にそのパケット内の見出し情報を走査するに過ぎない。顧客装置は、暗号処理を要求するのかが否かを見出し内に指示することを要求される。暗号処理を要求していることを指示している見出しフィールドを受信パーザ28が検出すると、データパケットは適切な部分が暗号エンジン22を通して進路変更される。パーザ28は1以上の異なるパケットフォーマットを認識し、各フォーマット内の暗号処理を要求していることを指示するコードを検出するように設計することができる。パーズングは、パケット内の暗号処理を開始すべき開始点の決定をも含む。暗号処理は、例えばデータ暗号化標準によるデータフレームの指定された部分の暗号化、またはデータパケットに追加するために完全性検査値(ICV)と呼ばれるフレーム検査シーケンス(または検査合計)の計算、または両者を含む。

【0030】送信パーザ30は、回路網側から到来するどのパケットを暗号処理するのかが決定する。この場合もパーズング機能は、フレーム見出し情報を走査し、この見出し情報に基づいて決定を行うのである。もしある到来パケットに対して暗号処理が要求されていれば、そのパケットの適切な部分が暗号エンジン22に向けられる。通常、到来パケットの処理は解読、または単にデータの完全性を保証するためのフレーム検査シーケンスの再計算を含む。

【0031】以上の説明から、本発明が回路網通信の暗号処理の分野に重要な前進を提供していることが理解されたであろう。具体的には、本発明は単一の暗号エンジンを使用してはいるが付加的な待ち時間を導入することなく、また処理能力に影響を与えることなく、回路網と

14

顧客装置との間に転送されるメッセージトラフィックの暗号処理に、複雑さを軽減させた手法を提供しているのである。例示の目的から、本発明の実施例の詳細を説明したが、本発明の思想及び範囲から逸脱することなく種々の変更を施すことができよう。従って、本発明は特許請求の範囲を除いて上記説明に限定されるものではないことを理解されたい。

【図面の簡単な説明】

【図1】顧客インタフェースと通信回路網との間に接続され、単一の暗号エンジンだけを有する本発明の実施例の暗号装置のブロック線図。

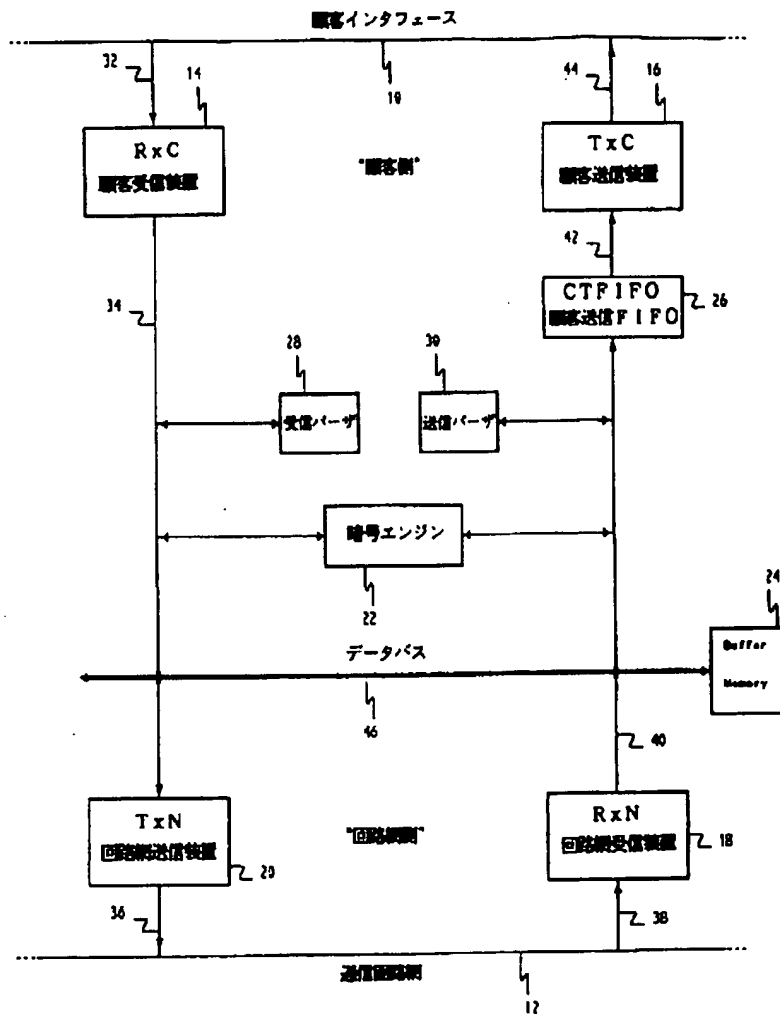
【図2】図1に類似した簡易化ブロック線図。

【図3】図1及び2に類似したより詳細なブロック線図。

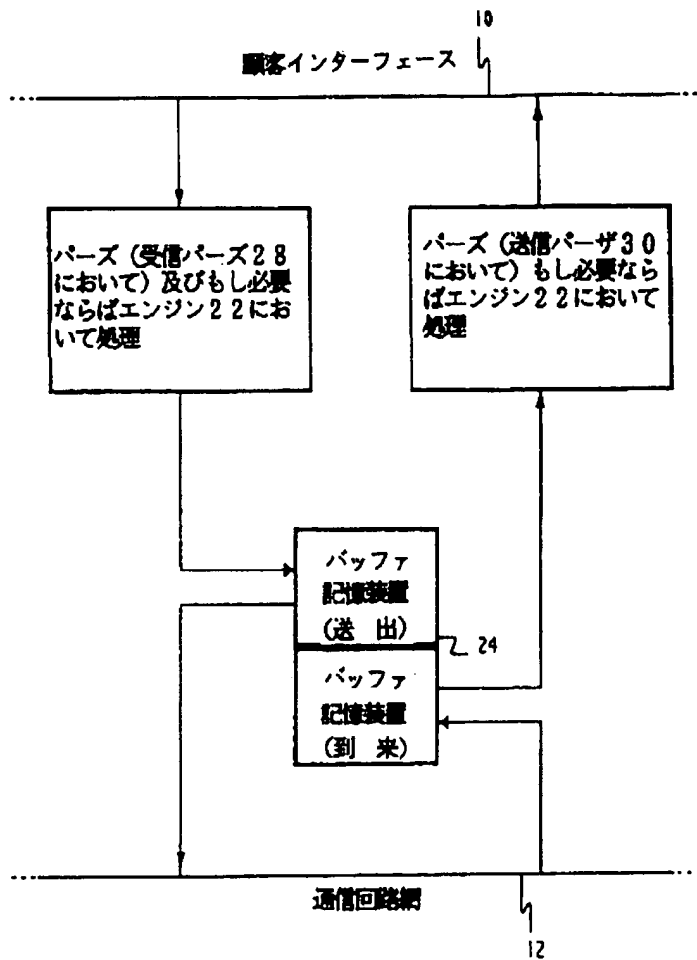
【符号の説明】

- 10 顧客インタフェース
- 12 通信回路網
- 14 顧客受信装置
- 16 顧客送信装置
- 18 回路網受信装置
- 20 回路網送信装置
- 22 暗号エンジン
- 24 バッファ記憶装置
- 26 顧客送信FIFO記憶装置
- 28 受信パーザ
- 30 送信パーザ
- 46 データバス
- 50 記憶装置制御装置
- 52 顧客受信制御論理回路
- 54 顧客送信制御論理回路
- 56 パケット制御論理回路
- 57、58、60、62 直接メモリアクセスユニット
- 64、66、68 付加FIFO記憶装置

【図1】



【図2】



【図3】

